Data Encryption by AES: Security Guarantee for Network Communication Sensitive Information

Jizhou Shan and Hong Ma
(Corresponding author: Jizhou Shan)

Hainan College of Economics and Business
Haikou, Hainan 571127, China
Email: shanji9125180@yeah.net

(Received Sept. 4, 2022; Revised and Accepted July 28, 2023; First Online Oct. 11, 2023)

Abstract

Encryption of data is an effective means of securing network communication. This paper briefly introduced the advanced encryption standard (AES) algorithm. It utilized the Rivest, Shamir, and Adleman (RSA) algorithm for encrypting the AES key to enhance the encryption process's efficiency. Then, the encryption and decryption efficiency, transmission efficiency, and security of the RSA, AES, and RSA+AES algorithms were compared using the simulation experiments. It was found that the increase in the size of transmission files increased the encryption and decryption time and reduced the average transmission rate. In terms of security, all three encryption algorithms had encryption sensitivity, and the RSA+AES algorithm had the best security performance in encrypting sensitive information.

Keywords: Advanced Encryption Standard; Information Protection; Network Communication; RSA Cryptosystem

1 Introduction

With the advancement and widespread use of computers and the Internet, communication between individuals has transcended traditional face-to-face interactions and letter writing [15]. The Internet enables seamless sending and receiving of emails, and real-time communication has become easily achievable due to the improvement in Internet transmission speeds. The Internet has significantly facilitated interpersonal communication [17]. However, the openness of the Internet also brings forth the risk of information theft or tampering during data transmission. Thus, safeguarding sensitive information during network communication has become a critical concern. Encryption of communication data is a widely adopted method to protect sensitive information, as it uses a key to transform plaintext into ciphertext, ensuring that even if intercepted, the data remains challenging to decipher [13, 14].

Several related studies have explored encryption techniques to enhance security. For instance, by using the advanced encryption standard (AES) for data compression and increasing the number of rounds in the AES encryption and decryption operations to 16, Kumar *et al.* [11] improved the security of a system. Yang *et al.* [22] developed an enhanced AES encryption algorithm based on chaos theory to address security concerns. They verified its feasibility and security through simulations. Albahar *et al.* [2] introduced a new triple algorithm combining Rivest, Shamir, and Adleman (RSA) [5, 8], AES, and TwoFish to further enhance the security of Bluetooth [9, 21], whose latest versions solely rely on 128-bit AES encryption.

Experimental data confirmed that the new algorithm eliminated all known weaknesses to improve the Bluetooth's encryption security. In this context, this paper offers a concise introduction to the AES encryption algorithm and suggests incorporating the RSA algorithm to encrypt the AES key, thus optimizing the encryption process. Subsequently, the study compares the encryption and decryption efficiencies, data transmission efficiencies, and security of three encryption algorithms, namely RSA, AES, and RSA+AES, through simulation experiments.

2 AES-based Encryption for Network Communication

In asymmetric cryptography, the public key is made available to the public, and anyone can access it to perform encryption [6, 10, 12, 20]. However, the private key is kept confidential by the individual, making it more secure. Symmetric encryption technology remains one of the commonly used mainstream cryptographic approaches due to its advantages of fast encryption, strong scalability, flexibility, and compatibility [19].

The fundamental process of the symmetric encryption algorithm AES comprises three main parts: key expan-

sion, encryption, and decryption. During the encryption process, the data is divided into several blocks, each consisting of four bytes. The initial round involves performing a bitwise exclusive OR (XOR) operation on the plaintext and the first round key. Subsequently, following the AES encryption algorithm rules, several rounds of iterations are conducted using the output of the initial round as input, culminating in the final ciphertext after the last round of iteration [7]. The decryption process follows a similar procedure to encryption but utilizes the round keys in reverse order. The AES algorithm is more efficient in both encryption and decryption processes; however, it also poses a higher risk of key leakage [3]. While the RSA algorithm provides greater security, its longer key length leads to decreased encryption efficiency. Hence, this article proposes combining AES and RSA by utilizing RSA for encrypting the AES keys. This approach not only mitigates the risk of leaking AES keys but also prevents unnecessary prolongation of the encryption process.

The process when the RSA and AES algorithms are combined is shown in Figure 1.

1) An AES key with 128 bits is used to encrypt the plaintext. The basic principle is as follows. A 128-bit plaintext and the key are put into a matrix of 4×4 respectively. Then, the key matrix and the plaintext matrix are subjected to the XOR operation [4]. After that, the S-box of the fixed table of the AES algorithm is utilized for byte replacement in the matrix. After the byte replacement, the matrix shifts the elements of each row to the left in a circular manner based on the specified displacement amount, which is called row shifting. Then, the column mixing operation is performed. The above procedure [16] is cycled nine times, and the column mixing is replaced by XOR operation at the tenth cycle.

2) The RSA public key is employed to encrypt the AES key. The encryption formula is:

$$\begin{cases} C = m^e \bmod n \\ \gcd[e, \phi(n)] = 1 \\ \phi(n) = (p-1)(q-1) \\ n = pq \end{cases} \tag{1}$$

where C is the ciphertext, m is the plaintext, e is the public key, p and q are two confidential prime numbers with random 1024 bits, and n is the product of p and q [18], which can be made public.

3) The communication ciphertext is combined with the ciphertext of the AES key at the communication sender, and then the combination is sent to the communication receiver.

4) The communication receiver splits the received combined ciphertext into communication ciphertext and AES key ciphertext.

5) The AES key ciphertext is decrypted using the RSA private key. The decryption formula is:

$$\begin{cases} m = c^d \bmod n \\ ed = 1 \bmod \phi(n) \end{cases} \tag{2}$$

where d is the private key, which is computed by the public key and is not public.

6) The decryption process uses the round keys in reverse order.

3 Simulation Experiment

3.1 Experimental Environment

The simulation experiments were conducted in a server in the lab, where three servers were set up. Server 1 served as the communication sender, server 2 served as the communication receiver, and server 3 acted as a third party to capture the communication data.

3.2 Experimental Setup

In the simulation experiment, servers 1 and 2 were used to establish a server-client architecture. Server 1 initiated communication while server 2 received it. The basic process is as follows. Firstly, servers 1 and 2 performed a handshake [23] to establish a unified AES key for encryption, and then they communicated with each other. Server 1 read the file that needs to be sent and encrypted it using an AES key; then, RSA encrypted the key and sent both the encrypted file and key to server 2. Finally, server 2 received the ciphertext and decrypted it.

3.3 Experimental Projects

1) Data encryption and decryption efficiency
Files with sizes of 100, 200, 300, 400, and 500 MB were set to test the encryption and decryption time. Additionally, the encryption and decryption time of both AES and RSA schemes was also tested.

2) Data transmission rate test
Files with sizes of 100, 200, 300, 400, and 500 MB were set up respectively, and they were encrypted and sent to the client according to the communication flow described above. The average transmission rate was calculated from the time when the server started sending the file to the time when the client finished receiving the file. In addition, the average transmission rate under the AES and RSA schemes was also tested.

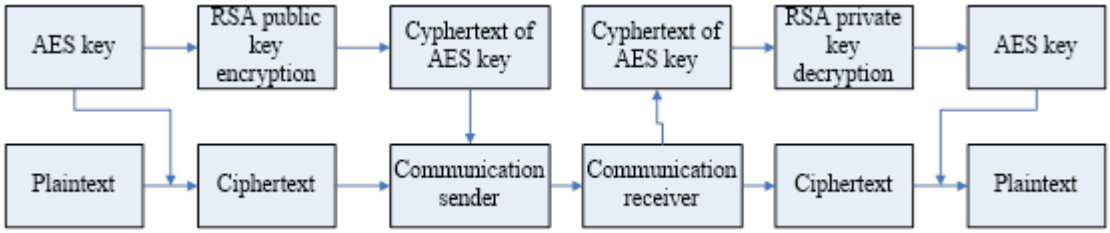

Figure 1: Communication encryption flow of the improved AES algorithm

3) Security of data encryption
In the process of communication between the server and client, the third-party server used the wiershark packet capture tool to simulate the listening condition and captured the communication data. In this test, the communication content was "hello", "hella", "nello", and the data captured by the packet capture tool was compared with the sent data.

4) Encryption effect on sensitive data
When encrypting communication data, sensitive information within it is also encrypted. Sensitive information includes the name, address and contact information of the communication user, so the encryption effect of the encryption scheme on the sensitive information was also tested. Firstly, 30 names, addresses and contact information were randomly generated, and then the sensitive information was transmitted under the three encryption schemes. The communication data was captured using a packet capture tool and violently decrypted for 60 min, and the decrypted text was compared with the original text to calculate the average completeness.

3.4 Experimental Results

The time required for encryption and decryption of the three encryption schemes is provided in Table 1. Comparing the encryption and decryption time consumed by the three encryption schemes under the same file size, it can be seen that the time consumed by the RSA algorithm was the most, the time consumed by the AES algorithm was the least, and the combination of the RSA and AES algorithms was slightly higher than the AES scheme. The RSA algorithm is a type of encryption algorithm that employs a public key to encrypt data and a corresponding private key for decryption purposes. The calculation method used in encryption and decryption is different, and moreover the calculation process both involves exponential operations. Therefore, it is the most time-consuming. The AES algorithm uses a key to encrypt and decrypt. The process of decrypting is the opposite of the process of encrypting, and the arithmetic process does not involve complex calculations. Therefore, it takes the least time. The RSA + AES algorithm encrypts plaintexts with the AES algorithm in nature, and the RSA algorithm is only applied to protect the AES key; therefore, the encryption and decryption by the combination algorithm is still faster than the RSA algorithm. However, encrypting the AES key with the RSA algorithm will take some time. As the length of the AES key is much smaller than the plaintext, the impact is not very large.

As can be seen from Figure 2, as the file size grew larger, the time for encryption at the server side and decryption at the receiver side in the communication process increased, making the average transmission rate decrease. Under the same file size, the average transmission rate of the RSA scheme was the smallest, the average rate of the AES scheme was the largest, and the average rate of the RSA+AES scheme was slightly lower than that of the AES scheme. The reason also lies in the difference of encryption efficiency of the encryption scheme. The RSA algorithm takes the longest time for encryption, which makes the average transmission rate low. The AES and combination algorithms take shorter time in encrypting and decrypting data, so the average transmission rate is high. Compared to the AES algorithm, the encryption and decryption of the combination algorithm take a little bit more time, which makes its average transmission efficiency slightly lower.

Under the three encryption schemes, the packet capture program was used to capture the transmitted data during the communication process. The captured data content, plaintext, and average completeness after brute-force decryption are demonstrated in Table 2. From Table 2, it is evident that the data bytes encrypted by the encryption algorithm were significantly different from the plaintext. In the same encryption algorithm, the difference of only one letter in the plaintext could make a significant difference in the ciphertext, and all three encryption algorithms had encryption sensitivity.

The cracking completeness of the three sensitive data such as name, address, and contact information after 60 min of brute force cracking under the three encryption schemes is displayed in Table 3. From Table 3, it can be seen that the average cracking completeness of the three sensitive data under the same encryption scheme did not differ much, and the comprehensive cracking completeness of the AES algorithm was the highest, the RSA algorithm was the second, and the RSA+AES algorithm was the lowest.

Table 1: The encryption and decryption time of three encryption schemes

Encryption scheme	100 MB	200 MB	300 MB	400 MB	500 MB
Time consumption of encryption and decryption by RSA/ms	740	950	1140	1320	1530
Time consumption of encryption and decryption by AES/ms	520	680	870	1020	1130
Time consumption of encryption and decryption by RSA+AES	580	730	890	1070	1190

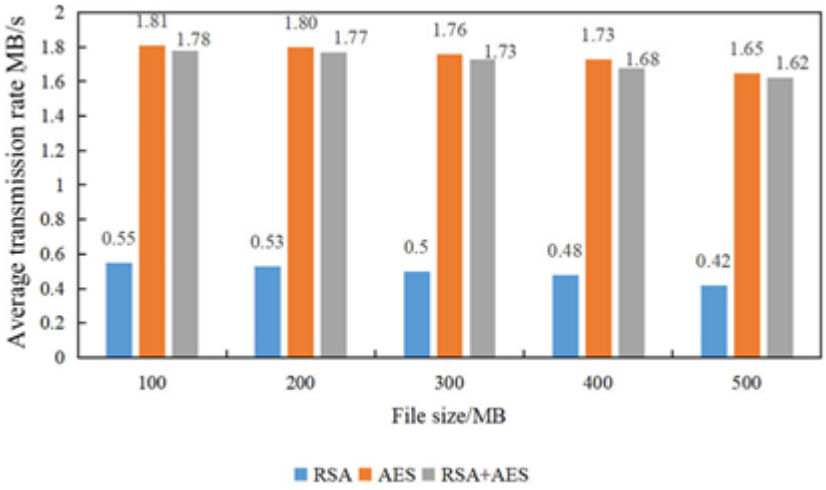

Figure 2: Average transmission rate of files of different sizes under three encryption schemes

Table 2: Data content captured under three encryption schemes

Encryption algorithm	Plaintext	Plaintext hexadecimal bytes	Captured data
RSA	hello	68656C6C6F	13551364da64d6355233
	hella	68656C6C61	20d5366d2gde2141da23
	nello	6E656C6C6F	635dg2e5f62314dde212
AES	hello	68656C6C6F	587a55a21ef56ac5dd54
	hella	68656C6C61	98a85d65ec6f54a55723
	nello	6E656C6C6F	7456fcea544f4dc44ef4d
RSA+AES	hello	68656C6C6F	3484ada8818461da4154
	hella	68656C6C61	7dfa2a45d5646654da11
	nello	6E656C6C6F	369a5f32587df1256564

Table 3: Brute force decryption completeness for different sensitive data types under three encryption schemes

Encryption scheme	Types of Sensitive Data	Average Cracking Completeness/%	Comprehensive Cracking Completeness/%
RSA	Name	3.2	3.2
	Address	3.1	
	Contact information	3.3	
AES	Name	4.2	4.1
	Address	4.1	
	Contact information	4.1	
RSA+AES	Name	2.1	2.1
	Address	2.2	
	Contact information	2.1	

4 Conclusion

This paper offers a brief overview of the AES encryption algorithm and incorporated the RSA algorithm to encrypt the AES key, aiming to enhance the encryption algorithm's performance. Subsequently, it conducted simulation experiments to compare the encryption and decryption efficiency, transmission efficiency, and security of three encryption algorithms: RSA, AES, and RSA+AES. The results are summarized as follows.

1) With the increase of the file size in the transmission, the encryption and decryption time for all three encryption schemes rose. When the file size was the same, RSA encryption and decryption required the most time, whereas AES encryption and decryption required the least amount of time. The RSA+AES algorithm showed slightly higher time consumption compared to the AES algorithm for the same file size.

2) As the number of transmitted files increased, the average transmission rate of the three encryption schemes showed a decreasing trend. Under the same file size, the RSA scheme had the smallest average transmission rate, while the AES scheme exhibited the largest average transmission rate. The average transmission rate of the RSA+AES scheme was slightly lower than that of the AES scheme.

3) All three encryption algorithms were cryptographically sensitive, meaning that even a minor change in the plaintext can result in a substantial change in the ciphertext.

4) Regarding the average completeness after 60 minutes of brute force decryption attempts, the AES encrypted ciphertext achieved the highest completeness upon decryption, followed by the RSA algorithm. The RSA+AES algorithm had the lowest completeness level.

References

[1] F. A. Abdulatif, M. Zuhiar, "Improve security of cloud storage by using third parity authentication, one time password and modified AES encryption algorithm," *International Journal of Informatics and Communication Technology*, vol. 7, no. 1, pp. 24-30, 2018.

[2] M. A. Albahar, O. Olawumi, K. Haataja, P. Toivanen, "Novel hybrid encryption algorithm based on AES, RSA, and Twofish for bluetooth encryption," *Information Security*, vol. 9, no. 2, pp. 168-176, 2018.

[3] N. Attar, H. Deldari, M. Kalantari, "AES encryption algorithm parallelization in order to use big data cloud Naser Attar, Hossein Deldari, Marzie Kalantari," *Computer and Information Science*, vol. 10, no. 3, pp. 23-28, 2017.

[4] A. Banushri, R. A. Karthika, "A survey on data security using file hierarchy attribute-based encryption in cloud computing environment," *Journal of Advanced Research in Dynamical & Control Systems*, vol. 2017, no. 4, pp. 144-149, 2017.

[5] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[6] Y. Feng, Y. Liu, G. Zhao, M. Xia, "An improved AES encryption algorithm based on the Hénon and Chebyshev chaotic map," *International Journal of Simulation: Systems, Science & Technology*, vol. 17, no. 48, pp. 25.1-25.8, 2016.

[7] R. Hamamreh, E. Tabib, "Selective image compression-encryption algorithm using adaptive Huffman coding and AES," *Journal of Applied Information Technology*, vol. 99, no. 4, pp. 932-945, 2021.

[8] M. S. Hwang, K. F. Hwang, I. C. Lin, "Cryptanalysis of the batch verifying multiple RSA digital signatures", *Informatica*, vol. 11, no. 1, pp. 15-18, Jan. 2000.

[9] M. S. Hwang, C. C. Lee, J. Z. Lee, C. C. Yang, "A secure protocol for bluetooth piconets using el-

liptic curve cryptography", *Telecommunication Systems*, vol. 29, no. 3, pp. 165-180, 2005.

[10] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73-84, 2004.

[11] P. Kumar, S. B. Rana, "Development of modified AES algorithm for data security," *International Journal for Light and Electron Optics*, vol. 127, no. 4, pp. 2341-2345, 2016.

[12] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[13] C. C. Lee, H. C. Tseng, C. C. Liu, H. J. Chou, "Using AES encryption algorithm to optimize high-tech intelligent platform," *WSEAS Transactions on Business and Economics*, vol. 18, pp. 1572-1579, 2021.

[14] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245-255, 2003.

[15] A. Mersaid, T. Gulom, "The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1," *Information Engineering*, vol. 4, no. 1, pp. 1-11, 2016.

[16] P. R. More, S. Y. Gaikwad, "An advanced mechanism for secure data sharing in cloud computing using revocable storage identity based encryption," *International Journal of Engineering Business Management*, vol. 1, no. 1, pp. 12-14, 2017.

[17] S. Oukili, S. Bri, "Hardware implementation of AES algorithm with logic S-box," *Journal of Circuits Systems & Computers*, vol. 26, no. 9, pp. 1-19, 2017.

[18] T. Paka, S. Divya, "Data storage security and privacy in mobile cloud computing using hierarchical attribute based encryption (HABE)," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 6, pp. 750-754, 2019.

[19] N. Rachmat, Samsuryadi, "Performance analysis of 256-bit AES encryption algorithm on Android smartphone," *Journal of Physics: Conference Series*, vol. 1196, 2019.

[20] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61-71, Mar. 2004.

[21] H. W. Yang, J. Z. Lee, M. S. Hwang, "A taxonomy of bluetooth security", *International Journal of Electronics and Information Engineering*, vol. 12, no. 2, pp. 43-65, 2020.

[22] Z. H. Yang, A. H. Li, L. L. Yu, S. J. Kang, M. J. Han, Q. Ding, "An improved AES encryption algorithm based on chaos theory in wireless communication networks," in *Third International Conference on Robot, Vision and Signal Processing (RVSP'15)*, pp. 159-162, 2015.

[23] H. Yue, X. Zheng, "Research on encrypting accounting data using des algorithm under the background of microprocessor system," *Microprocessors and Microsystems*, vol. 104061, 2021.

Biography

Jizhou Shan is an associate professor working on Technology for computer applications in the School of Information Technology in Hainan College of Economics and Business,China.He graduated from Northeastern University.His research interests include Computer network and Simulation,more than 30 papers published.

Hong Ma is an professor working on Technology for computer applications in the School of Information Technology in Hainan College of Economics and Business,China.He graduated from Northeastern University. Her research interests include Computer Technology.